Executive Summary

Protecting and ensuring the resiliency of the critical infrastructure and key resources (CIKR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. Attacks on CIKR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Attacks using components of the Nation's CIKR as weapons of mass destruction could have even more devastating physical and psychological consequences.

1 Introduction

The overarching goal of the National Infrastructure Protection Plan (NIPP) is to:

> ***Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.***

The NIPP provides the unifying structure for the integration of existing and future CIKR protection efforts and resiliency strategies into a single national program to achieve this goal. The NIPP framework supports the prioritization of protection and resiliency initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters. The NIPP risk management framework recognizes and builds on existing public and private sector protective programs and resiliency strategies in order to be cost-effective and to minimize the burden on CIKR owners and operators.

Protection includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links. In the context of the NIPP, this includes actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident (see figure S-1). Protection can include a wide range of activities, such as improving security protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, implementing cybersecurity measures, training and exercises, business continuity planning, and restoration and recovery actions, among various others.

Achieving the NIPP goal requires actions to address a series of objectives, which include:

- Understanding and sharing information about terrorist threats and other hazards with CIKR partners;
- Building partnerships to share information and implement CIKR protection programs;

Figure S-1: Protection

- Implementing a long-term risk management program; and
- Maximizing the efficient use of resources for CIKR protection, restoration, and recovery.

These objectives require a collaborative partnership among CIKR partners, including: the Federal Government; State, local, tribal, and territorial governments; regional coalitions; the private sector; international entities; and nongovernmental organizations. The NIPP provides the framework that defines a set of flexible processes and mechanisms that these CIKR partners will use to develop and implement the national program to protect CIKR across all sectors over the long term.

2 Authorities, Roles, and Responsibilities

The Homeland Security Act of 2002 provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation's CIKR. The act assigns DHS the responsibility for developing a comprehensive national plan for securing CIKR and for recommending the "measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities."

The national approach for CIKR protection is provided through the unifying framework established in Homeland Security Presidential Directive 7 (HSPD-7). This directive establishes the U.S. policy for "enhancing protection of the Nation's CIKR" and mandates a national plan to actuate that policy. In HSPD-7, the President designates the Secretary of Homeland Security as the "principal Federal official to lead CIKR protection efforts among Federal departments and agencies, State and local governments, and the private sector" and assigns responsibility for CIKR sectors to Federal Sector-Specific Agencies (SSAs) (see table S-1). It also provides the criteria for establishing or recognizing additional sectors. In accordance with HSPD-7, the NIPP delineates the roles and responsibilities for partners in carrying out CIKR protection activities while respecting and integrating the authorities, jurisdictions, and prerogatives of these partners.

Primary roles for CIKR partners include:

- **Department of Homeland Security:** Coordinates the Nation's overall CIKR protection efforts and oversees NIPP development, implementation, and integration with national preparedness initiatives.
- **Sector-Specific Agencies:** Implement the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CIKR sectors.
- **Other Federal Departments, Agencies, and Offices:** Implement specific CIKR protection roles designated in HSPD-7 or other relevant statutes, executive orders, and policy directives.
- **State, Local, Tribal, and Territorial Governments:** Develop and implement a CIKR protection program, in accordance with the NIPP risk management framework, as a component of their overarching homeland security programs.
- **Regional Partners:** Use partnerships that cross jurisdictional and sector boundaries to address CIKR protection within a defined geographical area.
- **Boards, Commissions, Authorities, Councils, and Other Entities:** Perform regulatory, advisory, policy, or business oversight functions related to various aspects of CIKR operations and protection within and across sectors and jurisdictions.
- **Private Sector Owners and Operators:** Undertake CIKR protection, restoration, coordination, and cooperation activities, and provide advice, recommendations, and subject matter expertise to all levels of government.
- **Homeland Security Advisory Councils:** Provide advice, recommendations, and expertise to the government regarding protection policy and activities.
- **Academia and Research Centers:** Provide CIKR protection subject matter expertise, independent analysis, research and development (R&D), and educational programs.

3 The CIKR Protection Program Strategy: Managing Risk

The cornerstone of the NIPP is its risk analysis and management framework (see figure S-2) that establishes the processes for combining consequence, vulnerability, and threat information to produce assessments of national or sector

Table S-1: Sector-Specific Agencies and Assigned CIKR Sectors

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture[a] Department of Health and Human Services[b]	Agriculture and Food
Department of Defense[c]	Defense Industrial Base
Department of Energy	Energy[d]
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water[e]
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration *United States Coast Guard*[f]	Transportation Systems[g]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities[h]

[a] The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[b] The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

[c] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DoD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

[d] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[e] The Water Sector includes drinking water and wastewater systems.

[f] The U.S. Coast Guard is the SSA for the maritime transportation mode.

[g] As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

[h] The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

risk. The risk management framework is structured to promote continuous improvement to enhance CIKR protection by focusing activities on efforts to: set goals and objectives; identify assets, systems, and networks; assess risk based on consequences, vulnerabilities, and threats; establish priorities based on risk assessments and, increasingly, on return-on-investment for mitigating risk; implement protective programs and resiliency strategies; and measure effectiveness. The results of these processes drive CIKR risk-reduction and management activities. The NIPP risk management framework is tailored to and applied on an asset, system, network, or mission essential function basis, depending on the fundamental characteristics of the individual CIKR sectors. DHS, the SSAs, and other CIKR partners share responsibilities for implementing the risk management framework.

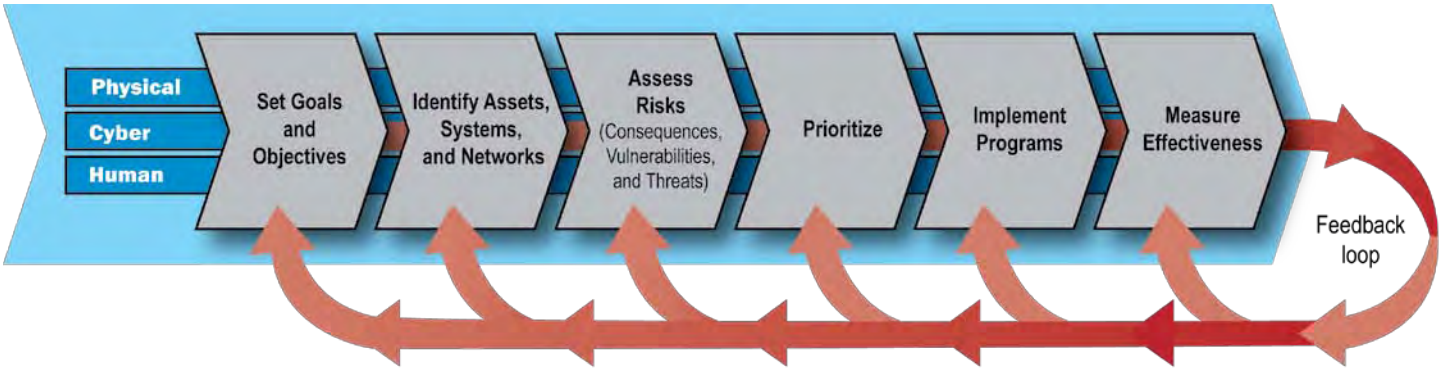
4 Organizing and Partnering for CIKR Protection

The enormity and complexity of the Nation's CIKR, the distributed character of our national protective architecture, and the uncertain nature of the terrorist threat and other manmade or natural disasters make the effective implementation of protection and resiliency efforts a great challenge. To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives.

The NIPP defines the organizational structures that provide the framework for coordination of CIKR protection efforts at all levels of government, as well as within and across sectors. Sector-specific planning and coordination are addressed through coordinating councils that are established for each sector. Sector Coordinating Councils (SCCs) comprise the representatives of owners and operators, generally from the private sector. Government Coordinating Councils (GCCs) comprise the representatives of the SSAs; other Federal departments and agencies; and State, local, tribal, and territorial governments. These councils create a structure through which representative groups from all levels of government and the private sector can collaborate or share existing approaches to CIKR protection and work together to advance capabilities. Engaging and coordinating with foreign governments and international organizations are also essential to ensuring the protection and resiliency of U.S. CIKR, both at home and abroad. The NIPP provides the mechanisms and processes necessary to enable DHS, the Department of State, the SSAs, and other partners to strengthen international cooperation to support CIKR protection activities and initiatives.

DHS works with cross-sector entities established to promote coordination, communications, and sharing of best practices across CIKR sectors, jurisdictions, or specifically defined geographical areas. Cross-sector issues are challenging to identify and assess comparatively. Interdependency analysis is often so complex that modeling and simulation capabilities must be brought to bear. Cross-sector issues and interdependencies are addressed among the SCCs through the CIKR Cross-Sector Council, which comprises the leadership of each of the SCCs. The Partnership for Critical Infrastructure Security provides this representation with support from the DHS CIKR Executive Secretariat. Cross-sector issues and interdependencies among the GCCs are addressed through the Government Cross-Sector Council, which comprises the NIPP Federal Senior Leadership Council (FSLC) and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). Additionally, the Regional Consortium Coordinating Council (RCCC) provides a forum for those with regionally based interests in CIKR protection.

Figure S-2: NIPP Risk Management Framework



Efficient information-sharing and information-protection processes based on mutually beneficial, trusted relationships help ensure implementation of effective, coordinated, and integrated CIKR protection programs and activities. Information sharing enables both government and private sector partners to assess events accurately, formulate risk assessments, and determine appropriate courses of action. The NIPP uses a network approach to information sharing that represents a new model for how CIKR partners share and protect the information needed to analyze risk and make risk-informed decisions. A network approach enables secure, multidirectional information sharing between and across government and industry. This approach provides mechanisms, using information-protection protocols as required, to support the development and sharing of strategic and specific threat assessments, threat warnings, incident reports, all-hazards consequence assessments, risk assessments, and best practices. This information-sharing approach allows CIKR partners to assess risks, identify and prioritize risk management opportunities, allocate resources, conduct risk management activities, and make continuous improvements to the Nation's CIKR protection posture.

NIPP implementation relies on CIKR information provided voluntarily by owners and operators. Much of this is sensitive business or security information that could cause serious damage to private firms, the economy, public safety, or security through unauthorized disclosure or access. The Federal Government has a statutory responsibility to safeguard CIKR protection-related information. DHS and other Federal agencies use a number of programs and procedures, such as the Protected Critical Infrastructure Information (PCII) Program, to ensure that security-related information is properly safeguarded.

The CIKR protection activities defined in the NIPP are guided by legal requirements such as those described in the Privacy Act of 1974 and are designed to achieve both security and protection of civil rights and liberties.

5 CIKR Protection: An Integral Part of the Homeland Security Mission

The NIPP defines the CIKR protection component of the homeland security mission. Implementing CIKR protection requires partnerships, coordination, and collaboration among all levels of government and the private sector. To enable this, the NIPP provides guidance on the structure and content of each sector's CIKR plan, as well as the CIKR protection-related aspects of State and local homeland security plans. This provides a baseline framework that informs the flexible and tailored development, implementation, and updating of Sector-Specific Plans; State and local homeland security strategies; and partner CIKR protection programs and resiliency strategies.

To be effective, the NIPP must complement other plans designed to help prevent, prepare for, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. Homeland security plans and strategies at the Federal, State, local, tribal, and territorial levels of government address CIKR protection within their respective jurisdictions. Similarly, CIKR owners and operators have responded to the increased threat environment by instituting a range of CIKR protection-related plans and programs, including business continuity and resilience and response measures. Implementation of the NIPP is coordinated among CIKR partners to ensure that it does not result in the creation of duplicative or costly risk management requirements that offer little enhancement of CIKR protection.

The NIPP, the National Preparedness Guidelines (NPG), and the National Response Framework (NRF) together provide a comprehensive, integrated approach to the homeland security mission. The NIPP establishes the overall risk-informed approach that defines the Nation's CIKR protection posture, while the NRF provides the approach for domestic incident management. The NPG sets forth national priorities, doctrine, and roles and responsibilities for building capabilities across the prevention, protection, response, and recovery mission areas. Increases in CIKR protective measures in the context of specific threats or that correspond to the threat conditions established in the Homeland Security Advisory System (HSAS) provide an important bridge between NIPP steady-state protection and the incident management activities under the NRF.

The NRF is implemented to guide overall coordination of domestic incident management activities. NIPP partnerships and processes provide the foundation for the CIKR dimension of the NRF, facilitating threat and incident management across a spectrum of activities, including incident prevention, response, and recovery. The NPG is implemented through the application of target capabilities during the course of assessment, planning, training, exercises, grants, and technical assistance activities. Implementation of the NIPP is both a national preparedness priority and a framework with which to achieve protection capabilities as defined by the NPG.

6 Ensuring an Effective, Efficient Program Over the Long Term

To ensure an effective, efficient CIKR protection program over the long term, the NIPP relies on the following mechanisms:

- Building national awareness to support the CIKR protection program, related protection investments, and protection activities by ensuring a focused understanding of all hazards and of what is being done to protect and enable the timely restoration of the Nation's CIKR in light of such threats;
- Enabling education, training, and exercise programs to ensure that skilled and knowledgeable professionals and experienced organizations are able to undertake NIPP-related responsibilities in the future;
- Conducting research and development and using technology to improve CIKR protection-related capabilities or to lower the costs of existing capabilities so that CIKR partners can afford to do more with limited budgets;
- Developing, safeguarding, and maintaining data systems and simulations to enable continuously refined risk assessment within and across sectors and to ensure preparedness for incident management; and
- Continuously improving the NIPP and associated plans and programs through ongoing review and revision, as required.

7 Providing Resources for the CIKR Protection Program

Chapter 7 describes an integrated, risk-informed approach used to: establish priorities, determine requirements, and guide resource support for the national CIKR protection program; focus Federal grant assistance to State, local, tribal, and territorial entities; and complement relevant private sector activities. At the Federal level, DHS provides recommendations regarding CIKR protection priorities and requirements to the Executive Office of the President through the National CIKR Protection Annual Report. This report is based on information about priorities, requirements, and related program funding information that is submitted to DHS by the SSA of each sector, the SLTTGCC, and the RCCC as assessed in the context of the National Risk Profile and national priorities. The process for allocating Federal resources through grants to State, local, and tribal governments uses a similar approach. DHS aggregates information regarding State, local, tribal, and territorial CIKR protection priorities and requirements. DHS uses these data to inform the establishment of national priorities for CIKR protection and to help ensure that resources are prioritized for protective programs that have the greatest potential for mitigating risk. This risk-informed approach also includes mechanisms to involve private sector partners in the planning process and supports collaboration among CIKR partners to establish priorities, define requirements, share information, and maximize risk reduction.